DoD IPv6 Context and Way Ahead

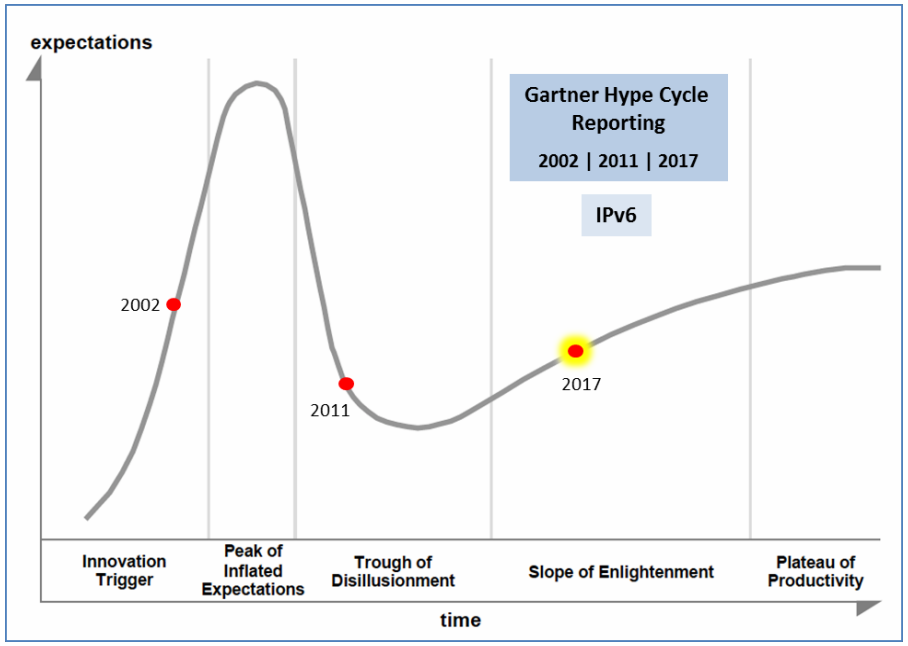
Col Keith Repik

Department of Defense

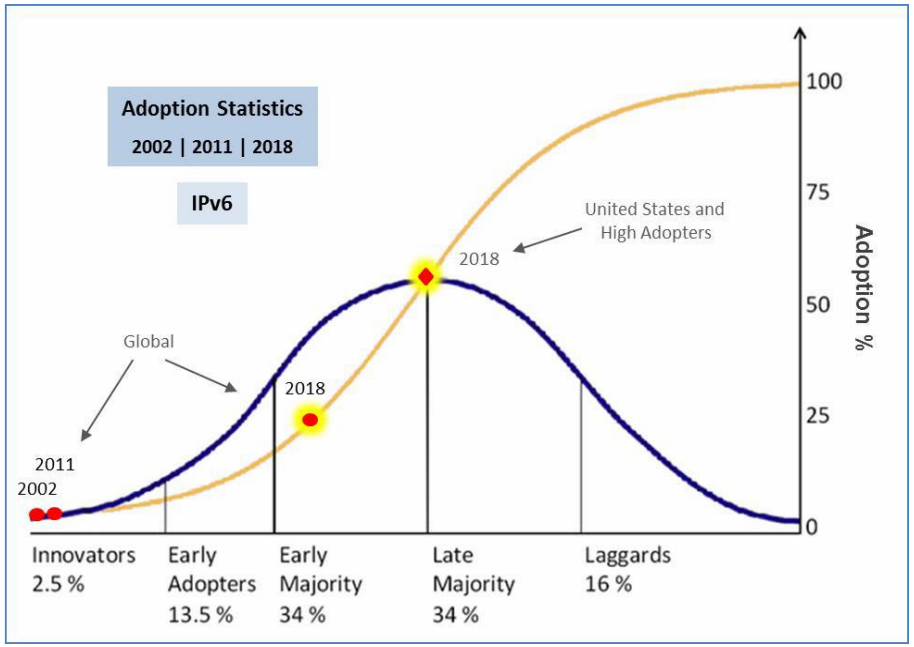
Office of the Chief Information Officer

13 Jun 2019

Context



No hype at this stage – quiet adoption and evolution



Core nations of global digital economy are here.

Context

IPv6 Preferred: *IPv4 as a Service*

Cellular

IPv6 Services Available

Cloud

Driving IPv6-Only Enterprise: Eliminate Dual Stack

Enterprise Networks

Demand Signals

Customers

No Strategy

5G capability will be enable and operationalized with IPv6

Innovative services and security approaches

IPv6 Enabled

Devices

IPv6 Required

Mobile Apps

Bi-Lingual: IPv4 and IPv6

Internet

IPv6 Preferred: 2020 - 2023

Residential/Business

High IPv6 Adoption: Interoperability

Mission Partners

*IPv6-enabled devices/software are already in our networks
*Determine acceptable use policies and standards – what does 'right' look like?
*Ensure sensors, analytics and automation are IPv6-aware

DoD Direction, Intent and Rationale

- DoD CIO memo signed 27 Feb 2019
- Initial direction and guidance:
  - Purpose: Reinvigorate preparations and planning
  - Focus: Long lead time actions and enabling capabilities
  - Key Priorities: cybersecurity, cloud, applications, mobility, mission partners
  - Goal: Secure and reliable IPv6 services in support of DoD missions
- ***Achieve meaningful and measurable progress over the next 2 years,*** and maintain sustainable course thereafter
- ***Reduce risk*** and ***enable opportunities***
- Multi-year effort to ***operationalize*** IPv6
  - People, processes, and technology … plus experience
- Provide agility and cybersecurity in support of global DoD operations and partnerships

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

FEB 27 2019

MEMORANDUM FOR CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
COMMANDANT OF THE COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: Internet Protocol Version 6 Implementation Direction and Guidance

Every computer, mobile phone, tablet, sensor and other networked device needs an Internet Protocol (IP) address to communicate with other devices and exchange data over the Internet. That need is growing rapidly with the continued expansion of 4G/5G mobile services, Internet access, cloud computing, virtualization, artificial intelligence and smart device usage. Unfortunately, nearly all of the 4.3 billion addresses provided by the current IP standard have been allocated since late 2015. As a result, global adoption of IPv6, its replacement, has risen steadily. IPv6 provides 340 trillion, trillion, trillion (i.e. undecillion) unique addresses and is thus key to the continued growth, development and evolution of information technology and services.

Many mobile service providers and wireline network operators have largely transitioned, and most mobile phones and computers are IPv6-enabled by default. New standards are optimizing for IPv6, and technology leaders such as Amazon, Google, Microsoft, Cisco and Facebook have mature implementation programs. Major corporations and governments are now establishing their transition strategies. Notably, China announced its goal to establish the world's largest IPv6 network in terms of scale, users, and traffic volume by the end of 2025.

Accelerating global adoption, increasing reliance on commercial solutions and services, mandates, growing DoD demand, and emerging technology and business trends necessitate DoD IPv6 capability. A proactive approach is essential as the necessary people, process and technology preparations to operationalize IPv6 take time and require experience. This memorandum therefore directs action and provides guidance in order to ensure unity of effort, achieve meaningful and measureable progress over the next two years, and sustain it thereafter.

The Department's goal is to provide secure and reliable IPv6 services in support of DoD missions. Key priorities include cybersecurity, cloud, mobility and mission partner interfaces. Major FY19-23 objectives contributing to the DoD goal include preparing unclassified DISN services and providing support for Internet-based capabilities.

To reinvigorate preparations, DoD Components will execute the actions specified in Attachment 1. The Joint Information Environment Executive Committee (JIE EXCOM) will ensure progress is sustained, and integration with other initiatives is achieved, in accordance with the JIE Management Charter. The DoD IPv6 Working Group will conduct integrated planning and provide support to the JIE EXCOM. The Department of Defense Chief Information Officer will conduct periodic reviews to monitor status and resolve challenges. The point of contact for this memorandum is Col Keith Repik, keith.a.repik.mil@mail.mil, (571) 372-7952.

Dana Deasy

Attachments:
As stated

DoD Direction, Intent and Rationale

Attachment 1

Direction and Guidance for IPv6 Implementation

The Department's goal is secure and reliable services in support of DoD missions. Initial priorities are cybersecurity, cloud, mobility and mission partner interfaces. Major FY19-23 objectives include preparing unclassified DISN services and support for Internet-based capabilities. Implementation will be accomplished in an orderly manner that ensures acceptable security and reliability. Initial direction and guidance for implementation is provided below:

(1) DoD CIO will:

a. Lead development of a DoD IPv6 Strategy for JIE EXCOM endorsement and DoD CIO signature NLT 4QFY19.
b. Determine DoD cybersecurity architecture and posture impacts using the DoD Cybersecurity Analysis and Review (DoDCAR) process NLT 1QFY20.
c. Integrate IPv6 considerations into the DoD Cyber Security Reference Architecture (CSRA) NLT 2QFY20.
d. Integrate IPv6 considerations into the DoD Core and Component Enterprise Data Center Reference Architectures NLT 4QFY19.
e. Determine US interagency collaboration and cybersecurity information sharing (e.g. best practices, product assessments and roadmaps) opportunities NLT 3QFY19.
f. Establish supplemental guidance for acquisition of IPv6-capable products in the Defense Acquisition Guidebook (DAG) and DoDIN Capabilities Requirements (DCR) document NLT 4QFY19.
   Note: Existing USG/DoD policy and the Federal Acquisition Regulation require acquisition of IPv6-capable products and services. The IPv6-capable definition requires support for both IPv4/IPv6 (i.e. dual stack) and IPv6-only environments. While IPv4 support is still required, IPv6-only capability (i.e. no IPv4-dependencies) is essential to minimize dual stack operations.
g. Propose Defense Federal Acquisition Regulation Supplement (DFARS) guidance for acquisition of IPv6-capable products NLT 4QFY19.

(2) Defense Information Systems Agency will:

a. Designate a DISA IPv6 lead and establish a virtual program management office.
b. Develop a DISN IPv6 Implementation Plan for FY19-23 within 90 days of this memo. Include required actions with proposed schedule, costs, milestones and critical dependencies to deliver reliable and secure IPv6 services within the DISN, and in support of Internet-based capabilities.
c. Provide an electronic means for DoD Components to submit, manage and de-conflict IPv6 priorities, plans and requirements NLT 3QFY19.
d. Provide on-demand IPv6 familiarization training and assess commercial advanced training resources for network engineers and cybersecurity personnel NLT 4QFY19.
e. Provide on-demand advanced IPv6 training resources for network engineers and cybersecurity personnel NLT 1QFY20.
f. Update and maintain IPv6 standards and implementation profiles in the Defense Information Technology Standards Registry (DISR) NLT 1QFY20.

g. Verify Internet Access Point (IAP) systems provide equivalent IPv4/IPv6 capabilities and resolve gaps. Provide POA&M(s) for any unresolved gaps NLT 1QFY20.
h. Verify the Secure Cloud Computing Architecture (SCCA) provides equivalent IPv4/IPv6 capabilities and resolve gaps. Provide POA&M(s) for any unresolved gaps NLT 1QFY20.
i. Verify DoD Public Key Infrastructure (PKI) provides essential IPv6 functionality (e.g. OCSP responder) for external facing services and resolve gaps NLT 2QFY20.
j. Develop test processes and methodologies to assess compliance with DCR-related IPv6 requirements for Approved Products List (APL) testing NLT 1QFY20.
k. Verify current STIGs/SRGs are consistent with IPv6-related cybersecurity requirements by 1QFY20.
l. Verify milCloud 2.0 provides equivalent IPv4/IPv6 capabilities and resolve gaps. Provide POA&M(s) for any unresolved gaps NLT 2QFY20.
m. Provide IPv6-enabled Cyber Security Range services NLT 1QFY20.
n. Provide Domain Name System services to IPv6-only users/networks for the .mil generic top level domain NLT 1QFY21.
o. Provide IPv6-enabled unclassified milCloud 2.0 services NLT 1QFY21.

(3) National Security Agency will:

a. Assist DISA in verifying that IAP systems provide equivalent IPv4/IPv6 capabilities.
b. Provide cybersecurity guidance in support of DoD IPv6 deployments as needed.
c. Provide technical input to updates and maintenance of IPv6 standards registries as needed.
d. Assist DISA with IPv6 training identification, assessment and development.
e. Provide IPv4/IPv6 Attack Sensing and Warning, and Cyber Threat Intelligence, NLT 1QFY21.

(4) United States Cyber Command will:

a. Establish requirements for IPv6 training and tools for Cyber Mission Force personnel NLT 1QFY20.

(5) DoD Components and the United States Coast Guard will:

a. IPv6-enable all commercially hosted public facing unrestricted services NLT 4QFY19. Monthly reporting will be accomplished with instructions to follow.
b. Identify DoD hosted public facing unrestricted services NLT 3QFY19. Include planned disposition (e.g. retain in place, transition to cloud by date, retire by date, etc.) and dependencies to enable IPv6.
c. Ensure new cybersecurity products provide equivalent IPv4/IPv6 capabilities.
d. Verify existing cybersecurity systems provide equivalent IPv4/IPv6 capabilities and resolve gaps. Provide POA&Ms for any unresolved gaps NLT 1QFY20.
e. Ensure all applications and systems migrated to commercially hosted cloud services are IPv6-only capable. If provider limitations exist, obtain a resolution roadmap.
f. Monitor and report mission partner IPv6 plans and status on a semi-annual basis, or earlier as needed. Use existing engagement forums where possible (e.g. CCEB).
g. Identify any additional resources required to support actions directed in this guidance, and incorporate into Program Objective Memorandum FY21 submissions.